REMARKS

Claims 1-7, 9-19, 21 and 22 are presented for further examination. Claims 1, 7, 9, 10, 13-19, and 21 have been amended. Claim 22 is new. No new matter has been added. Claims 6, 8, and 20 are canceled.

In reply to the Response After Final filed on April 19, 2010, the Examiner issued an Advisory Action dated May 4, 2010. In that Advisory Action, the Examiner indicated the Response filed on April 19, 2010, was entered but it did not place the claims in condition for allowance. Thus, claims 1-21 remain rejected under 35 U.S.C. § 103(a) as obvious over Mills (U.S. Patent No. 6,311,204) in view of Ducharme (U.S. Patent No. 7,165,180).

In remarks accompanying the Advisory Action, the Examiner explained that he believed Mills disclosed all of the claimed features except the on-chip storage of a secret key, which he felt was described in Ducharme. In response to arguments submitted by the applicants regarding the missing common key storage register for multiple decrypted common keys, the Examiner stated that such a register was within the skill of an artisan in this technology.

Applicants respectfully request reconsideration and further examination of the claims.

Claim Rejections

The present disclosure is directed to, *inter alia*, providing a more secure interface with a signal provider in order to eliminate or greatly reduce the risk of unauthorized access to sensitive information at the interface. To do this, the present circuit eliminates all non-encrypted inputs. It receives a secure broadcast signal along with encrypted control words and encrypted common keys. What enables the circuit to decrypt the signals in a secure manner for processing and ultimate use is the on-chip storage of a secret key. This secret key is used to decrypt the common keys, which in turn are used to decrypt the control words, which in turn are used to decrypt the broadcast signal.

A feature of the present circuit is the decryption and storage of multiple common keys that are retained in a storage register for use with associated respective programs. Each decrypted common key is associated with one or more respective broadcast signals or programs

by a program identifier. This enables the broadcast signal provider to offer different levels of service to its customers by providing limited or controlled access to the broadcast signals of programs.

A further feature is the use of a secret key that is unique to the particular circuit. In other words, the secret key remains permanently identified with only that particular circuit, and it does not change. On the other hand, the control words are changing relatively infrequently compared to the encrypted common keys, which change several times a month to several times an hour.

In remarks accompanying the Advisory Action, the Examiner states:

> In response to applicant's argument Examiner asserts that Ducharme's reference was used as a secondary reference to show that encryption key can be stored in clear form within the circuit itself. Miller [sic] is a primary reference which was cited for other limitations.

Applicants believe the Examiner's reference to a previous cited patent to Miller was in error and the Examiner intended to refer to Mills. Applicants respectfully assert that the combination of Mills and Ducharme does not teach or suggest the claimed combination recited in these amended claims.

Claim 1 is directed to a semi-conductor integrated circuit that comprises a monolithic circuit for decryption of encrypted broadcast signals, the monolithic circuit has an input interface that is structured to receive the encrypted broadcast signals, encrypted common keys, and encrypted broadcast control data having encrypted control signals and, *inter alia*, a first decryption circuit that outputs decrypted control signals to a processing unit by using a common key from a plurality of common keys stored in a common key store in association with a respective identifier corresponding to each broadcast signal. Claim 1 further recites a second decryption circuit that decrypts the common keys in accordance with a secret key from a secret key store in which the secret key is unique to the monolithic circuit. Because the secret key is unique to the monolithic circuit, there is no need to change the secret key. In contrast, the common keys are changed at a rate predetermined, which is recited in later claims.

Support for the foregoing amendments can be found in the specification beginning at page 8, line 9 and continuing through line 18. As stated therein, the use of multiple

common keys allows different levels of service to be provided depending on the service paid for and hence the keys provided.

There is no teaching or suggestion in either Ducharme or Mills of having a common key store structured to store a plurality of decrypted common keys in association with a respective identifier corresponding to each broadcast signal. There is also no teaching or suggestion in either Ducharme or Mills of having a secret key that is unique to the monolithic circuit and that is not accessible from outside the monolithic circuit. This can be seen, for example, in Figure 2 of the present application in which the secret key store 34 only communicates unidirectionally with the decryption circuit 32 via single line 35.

In view of the foregoing, applicants respectfully submit that claim 1 is clearly allowable over the references cited and applied by the Examiner.

Dependent claims 2-5 and 7 are allowable for the features recited therein as well as for the reasons why claim 1 is allowable. For example, claim 7 recites the integrated circuit having multiple identifiers associated with each common key. None of the references teaches or suggests having identifiers associated with any key much less multiple identifiers associated with each key.

Independent claim 9 is directed to a system that includes a transmitter that transmits the encrypted broadcast signals, encrypted control words, and encrypted common keys, with the common keys encrypted according to a unique secret key and the common keys associated with the respective encrypted broadcast signals with a respective identifier. Claim 9 also recites a common key store that stores a plurality of decrypted common keys with their associated identifiers. A second decryption circuit is also recited in which the common keys are decrypted in accordance with a secret key and are stored in the common key store with their respective identifier. Applicants respectfully submit that claim 9 is allowable, along with its dependent claim 22, for the reasons discussed above with respect to claim 1.

Independent claim 10 is directed to set top decoder service for decryption of broadcast signals that includes a monolithic device having a common key store configured to receive a decrypted common key and a respective identifier that is associated with a respective broadcast signal and further including a secret key store configured to store a secret key that is

unique to the monolithic device. A decryption unit decrypts the encrypted common key in accordance with a secret key and stores the decrypted common key in the common key store with the respective identifier that associates the decrypted common key with the respective broadcast signals. Neither Ducharme nor Mills, taken alone or in any combination thereof, teach or suggest these features in the context of a set top decoder device. Thus, claim 10 along with dependent claims 11 and 12 is clearly allowable over the references cited and applied by the Examiner.

Claim 13 is directed to a method of decrypting encrypted broadcast signals in which, *inter alia*, encrypted broadcast common keys are decrypted utilizing a stored secret key in the secret key store in the semiconductor integrated circuit to generate keys and program identifiers that associate each common key with a respective broadcast signal. The common key store is recited as storing the common keys with respective identifiers in a table format. Nowhere to Ducharme or Mills, taken alone or in any combination thereof, teach or suggest a method of decrypted encrypted broadcast signals that include the entire combination of steps as recited in claim 13 to include decrypting the encrypted common keys and storing them in a common key store with associated identifiers.

Dependent claim 14 and 15 are also allowable for the features recited therein as well as for the reasons why claim 13 is allowable. For example, dependent claim 15 recites changing the encrypted broadcast common keys at a rate that is in the range of more than once per hour. Support for this amendment can be found in the specification at page 8, lines 1-2, in which it states: "Thus, new common keys need to be broadcast at the rate of a few per hour."

Independent claim 16 is directed to a method for broadcasting signals to a plurality of subscribers as well as to receiving and decrypting those broadcast signals. Claim 16 includes the limitations discussed above with respect to claim 13 as well as the steps of encrypting control words associated with the broadcast signals and broadcasting the encrypted control words as well as encrypting common keys associated with the broadcast signals by program identifiers and broadcasting the same. Applicants respectfully submit that claim 16, as well as dependent claims 17 and 18, is allowable as discussed above with respect to claims 13-15.

Independent claim 19 is directed to a system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals. Claim 19 has been amended to recite the transmitter configured to change the encrypted common keys at a rate that is greater than once per hour. This feature along with the other features recited in claim 19, as discussed above with respect to claim 10, render claim 19 allowable over the combination of Mills and Ducharme.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are now in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jk

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1622426_1.DOC